What is claimed is:

1. A method for securing a communication comprising the steps of

assigning a first confidential key at a server for use by an originating subscriber gateway,

transmitting said first confidential password from said originating subscriber gateway to a terminating subscriber gateway in advance of or simultaneous with a first encrypted data packet, said first encrypted data packet being encrypted with said first confidential key, and

exchanging packets encrypted via said first confidential key between said originating and said terminating subscriber gateway.

2. A method as recited in claim 1 wherein said server assigns replacement first confidential keys at random intervals of time.

3. A method as recited in claim 1 wherein said server assigns replacement first confidential keys every N packets where N may be one or more.

4. A method as recited in claim 3 wherein an encrypted data packet contains a replacement first confidential key encrypted with the first confidential key and further comprises the step of decrypting the replacement first confidential key with the first confidential key, the replacement first confidential key being used to decrypt the next received encrypted data packet.

5. A method as recited in claim 1 comprising the steps of, after a predetermined period of time, the originating subscriber gateway signaling the terminating subscriber gateway to take control and the terminating subscriber gateway performing steps i through iii as a replacement originating subscriber gateway, the originating subscriber gateway becoming the terminating subscriber gateway.

6. A method for securing a communication as recited in claim 1 where the communication is a multimedia communication comprising audio, video and data and one of audio, video and data

are encrypted at a first level of security and another of audio, video and data are encrypted at a second level of security.

7. A method as recited in claim 1 comprising the step of receiving a second key from a user and transmitting said second key from said originating subscriber gateway to said terminating subscriber gateway, said originating and terminating subscriber gateway utilizing a two key encryption algorithm.

8. A method as recited in claim 1 further comprising the steps of receiving keys at an intermediate server from the originating and terminating gateway and an indication of the encryption algorithm utilized by each gateway and translating an encrypted message at said intermediate server between said originating and terminating gateways between one encryption algorithm and another.

9. A method as recited in claim 6 further involving a third party, the third party having access to a first level of security and not a second level of security, the third party capable of receiving one of audio, video and data and not receiving another of audio, video and data.

10. A method as recited in claim 6 further comprising the step of receiving changes input by a user in level of security in real time and effectuating such a change.

11. A method as recited in claim 1 further comprising the steps of said server downloading an encryption algorithm to said originating and terminating subscriber gateways.

12. A method as recited in claim 11 further wherein said downloading of an encryption algorithm occurs at random intervals during a communication.

13. A method as recited in claim 1 further comprising the initial step of said originating subscriber gateway registering with said server, the originating subscriber gateway receiving the first confidential key in response to completion of the registration step.

14. A method as recited in claim 13 further comprising the step of receiving a secure call command during a communication for one of audio, video, data and multimedia.

15 A system providing secure communications in an integrated broadband communication system, including:

a secured communication server providing security keys for encrypting and decrypting communication information; and

a first intelligent gateway that encrypts and decrypts packets of communication information using said security keys provided by said secured communication server in real time in response to user input during a communication session.

16. The system according to claim 15, further comprising a second intelligent gateway that encrypts and decrypts packets of communication using a security key received from said first intelligent gateway.

17. The system according to claim 16, wherein said first intelligent gateway is a customer gateway and said second intelligent gateway is a customer gateway.

18 The system according to claim 16, wherein said first intelligent gateway is a customer gateway and said second intelligent gateway is a gateway that couples said broadband communication system with another communication system.

19. The system according to claim 18, wherein said another communication system is a public switched telephone network.